Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 149 – 154

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment

Sheik Khadar Ahmad Manoj*, D.Lalitha Bhaskari

Department of Computer Science and Systems Engineering,Andhra University College of Engineering, Visakhapatnam-53003, India

Abstract

With the rapid growth of cloud adoption in both private and public sectors globally, cloud computing environment has become one of the prospective battle field for cyber attackers where one of the major challenges of cloud computing is the protection of data from various attacks. Mostly, Cloud services are provided by the service providers where data security is a major concern for the client. In this paper an attempt to provide a possible solution for such threats is proposed along with an exposure to various issues related to data security in cloud and the various challenges faced by forensic experts in cloud. A model based on trusted third party (TTP) along with a cloud forensics investigation team (CFIT) proves to be a better solution to enhance the trustworthiness of the service provider and thereby facilitate the cloud providers to trap cyber attackers with strong collection of evidences which might help in further legal process.

Peer-review under responsibility of the Organizing Committee of CMS 2016

Keywords: Cloud computing;Trusted Third party (TTP); Cloud forensics;Digital investigation;Cyber attacks.

1. Introduction

Cloud computing is a new IT phenomenon which is being widely adapted by many people around the globe. This adaption generated a security concern for the stored data in cloud environment. When security attacks or

* Corresponding author. Tel.: +91-8886854522;
*E-mail address:*skamanoj@gmail.com

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.202

policy violations occur, it makes necessary to conduct a digital forensic investigation. But, existing digital forensic principles, frameworks, practices and tools are largely intended for off-line investigation and in particular, these approaches assume that the storage media under investigation is completely within the control of the investigator[1]. Conducting investigations in a cloud computing environment presents new challenges which are to be addressed.

This paper proposes a frame to make the cloud environment reliable and preserve the trustworthiness of cloud service providers. This paper is organized into 5 sections where in section II overview of cloud computing is given. Section III deals with the introduction to cloud forensics and the challenges of forensics in cloud environment. In section IV a detailed explanation of the proposed frame work model is presented followed by conclusions in section V.

2. Cloud Computing

Cloud computing is continuously growing and emerging technology. The hardware and software resources that provide diverse services over the network or the internet to address the user requirements are called "Cloud". Here, resources refer to computing applications, network resources, platforms, soft ware services, virtual servers and computing infrastructure. The cloud computing can be conceived as pay-go-use model wherein the clients pay for the requested resources. Cloud computing eliminates the costs and complexity of buying, configuring and managing the hardware and software.

The cloud architecture mainly provides three categories of services [2] Iaas(Infrastructure as a Service), Paas(Platform as a Service) and Saas(Software as a Service)

The four well-known deployment models used in cloud computing are[2] Public Cloud, Private Cloud ,Hybrid Cloud and Community Cloud.

3. Cloud Forensics

A cyber criminal can be described as a person who legitimately involves in destruction of privacy or security of data and utilizing unauthorized resources causing loss to the digital users. Cloud computing environment is becoming a new battle field of cybercrime where new challenges are being posed to defend the cyber attacks. To meet the challenges of digital data threat, digital forensics methods[6] are applied over the remote servers of cloud giving way to a new term called "Cloud Forensics".

Basing on NIST Cloud Computing Reference Architecture[6], the researchers revisited the definition proposed in Ruan et al. 2011A, and proposed a working definition of cloud forensics as "Cloud forensics is the application of digital forensic science in cloud computing environments. Technically, it consists of a hybrid forensic approach towards the generation of digital evidence. Organizationally it involves interactions among cloud actors (i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) for the purpose of facilitating both internal and external investigations. Legally it often implies multijurisdictional and multi-tenant situations"

According to National Institute of Standards and Technology[4], the major challenges of Cloud Forensics are categorized into the following nine major groups which are summarised as

- Architecture (e.g., diversity, complexity, provenance, multi-tenancy, data segregation, etc.)
- Data collection (e.g., data integrity, data recovery, data location, imaging, etc.)
- Analysis (e.g., correlation, reconstruction, time synchronization, logs, metadata, timelines, etc.)
- Anti-forensics (e.g., obfuscation, data hiding, malware, etc.)
- Incident first responders (e.g., trustworthiness of cloud providers, response time, reconstruction, etc)
- Role management (e.g., data owners, identity management, users, access control, etc.)
- Legal (e.g., jurisdictions, laws, service level agreements, contracts, subpoenas, international cooperation, privacy, ethics, etc.)

- Standards (e.g., standard operating procedures, interoperability, testing, validation, etc.)
- Lack of Training (e.g., forensic investigators, cloud providers, qualification, certification, etc.)

This paper attempts to address the challenges related to Architecture and Incident first responders.

4 . Proposed Model

Any attack can be successfully thwarted by collective teamwork and meticulous planning. For a cyber attack to be recognized and to make it unsuccessful, a model based on collective actions of a group of authenticated members (actors) is explained in this section. The main actors and their roles in the proposed model are

i. *Cloud Customer* (CC): Cloud customer is the end user who benefits the cloud services. To have the advantages of cloud resources the CC should have a unique identity.

ii. *Trusted Third Party* (TTP): TTP is involved to help ensure identification and sort out the security breaches with occasional help from cyber forensics team.

iii. *Cloud Service Provider* (CSP): CSP is the owner of the servers and databases which he lends on rent basis, CSP should register itself to TTP in-order to offer services to CC's.

iv. *Cloud Forensics Investigation Team* (CFIT): The CFIT team will come into action when it receives a request from TTP to deal with suspicious activities in cloud. The CFIT is also have the privilege of using the latest tools as TTP will always have the latest updated versions of forensics software.

The model can be outlined as shown in the Figure 1and is followed by the brief explanation.

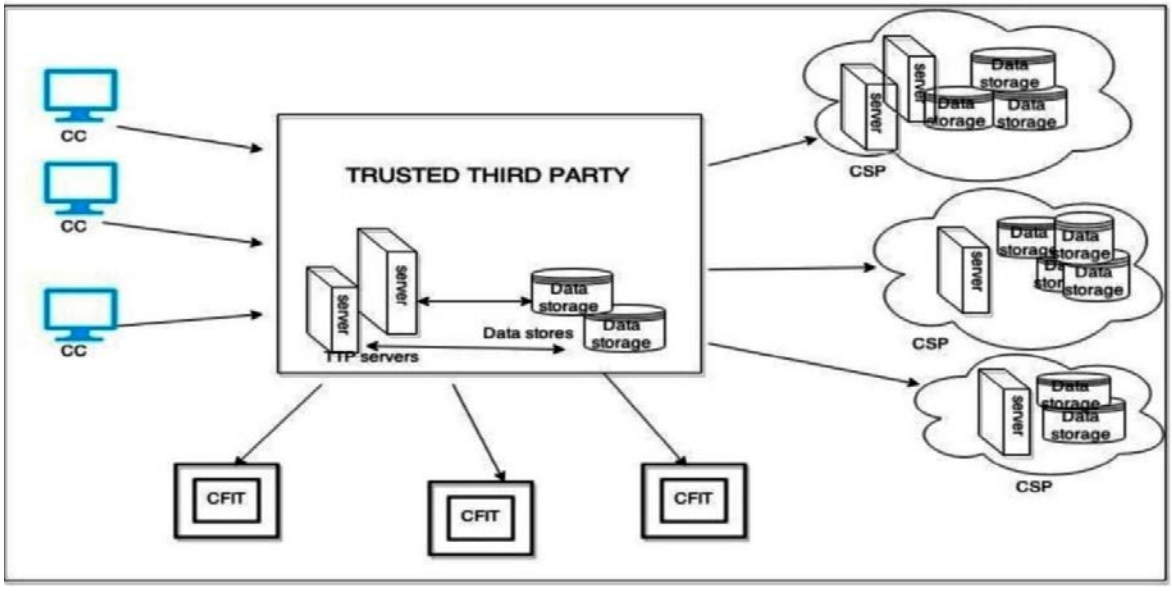

Fig.1. Outline of Proposed Model

TTP validates the integrity of several CSP's and register them as the trusted service providers with necessary paper work. The TTP will classify the CSP basing on the services they offer and locations where they reside. When a CC wants to use cloud services the person will approach to the TTP with a valid identity along with a list of requirements/services to be served by cloud. The TTP then explains all the rules and regulations need to be followed by CC and gets all necessary legal documents signed by CC to have the membership. The CC also gets the signed documents by TTP as per policy. When all the necessary proceedings are completed, the TTP provides the customer with login details to use the cloud services. Figure 2 explains the process of CC registration.

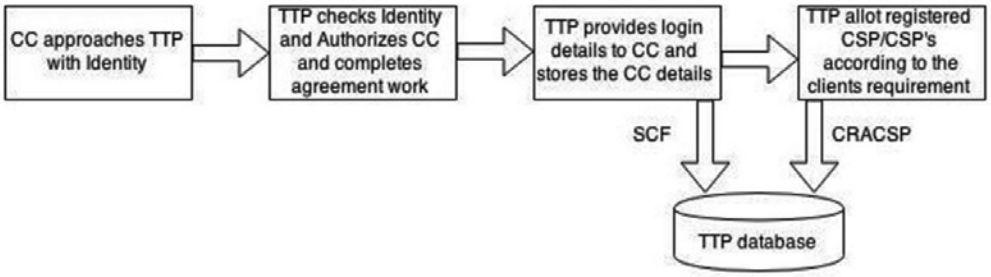

Fig.2. CC Registering process with TTP

The TTP will make a decision to which registered CSP/CSP's the client should be assigned corresponding to the requirements of CC and services offered by various CSP's. TTP creates a user account with the CSP on behalf of the CC and maintains a record of the same in its SCF (Secured Client File) along with Client Requirement Allotted CSP (CRACSP) as shown in table 1 and table 2, for future login process.

Table 1
Secured Client File (SCF)

Client Id	Login Details with TTP	I.P Address	Location

Table 2
Client Requirement Allotted CSP (CRACSP)

Client Id	Requirement Id	Allotted CSP	Login details with CSP

The CRACSP is required as all the client requirements are not supported by a single CSP so TTP would examine the client's requirements carefully and allot the CSP's accordingly. The two tables are stored by the TTP's internal database storage devices.

The TTP is associated with a group of CFIT's basing on their ratio of success in investigation of cases. CFIT's can be from both Government and recognised private agencies.

Now, the TTP becomes central authority of the cloud environment as CSP's are unaware of their CC's and vice versa. The total security and responsibility lies with TTP. The TTP ensures the privacy of CC

When a CC wants to enter the cloud, first step is to authenticate to TTP and get STT (short time ticket) generated and issued by the TTP.TTP sends the same STT is to the CSP. It also records this session details of the CC for future reference, the details of STT generation remains with TTP (The STT may be the hash over the details of the client and CSP like I.P address, time of generation, client ID, CSP ID or it may be the digital signature of TTP) and it will expire within a specified amount of time, so breaking it is not an easy task and hence authentication and security is taken care off.

TTP opens an interface to the client on behalf of CSP to preserve the identity of CSP so that a CC can never know to which CSP being connected to. The login details are redirected to CSP. The CSP will accept login from the CC only through the TTP by validating STT. Here, The TTP acts as a firewall to the CSP. This process is shown in the Figure 3.

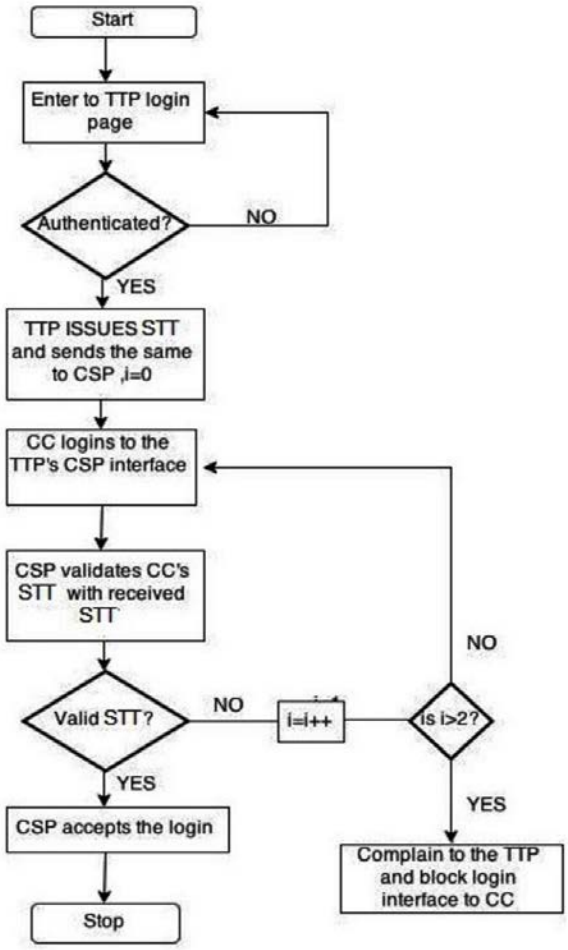

Fig. 3.Login process of CC

Whenever the TTP gets suspicion at the operational behaviour of CC/CSP or receives a complaint from the CC/CSP about security related issue's the TPP will alert the corresponding CFIT about the situation and assist them in the investigation process by providing the necessary information required from its tables (CRACSP and SCF). The CFIT has the following advantages

- As TTP provides time and location of CSP where the security breach occurred CFIT can capture the relevant image of the digital evidence
- The CFIT is provided with all the necessary updated software tools and suggestions for the CFIT as it is associated with many other CFIT's which makes the investigation in an efficient way.
- Once, data is collected the analysis process is done by other CFIT's in parallel to fasten the investigation.
- As, CFIT knows the I.P address and location from where the incident occurred, there is a great probability to identify and present the criminal in the court of law, within a short period of time.

5. Conclusion

As the digital world is rapidly transforming itself towards Cloud computing there is an alarming rise in cyber attacks hence leading to the development of effective security solutions for the cloud environment. This paper presents a frame work for establishing a secure cloud environment with the help of a team which consists of cloud customers, cloud providers, Trusted Third party and Forensic investigators. As the idea of TTP is already proved to be secure this model may prove to be a promising solution. One main concern would be about TTP as it is a single point contact node between all the other actors. This could be resolved by creating backups periodically.

References

1. Grispos, George, Tim Storer, and William Bradley Glisson. "*Calm before the storm: the challenges of cloud*." Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security 4 (2013): 28-48.
2 . http://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf
3. Liu, Fang, et al. "*NIST cloud computing reference architecture*." NIST special publication 500 (2011): 292.
4. "*Cloud Computing Forensic Science Challenges*", National Institute of Standards and Technology Interagency or Internal Report 8006,June 2014.
5. Ruan, K., Carthy, J.,Kechadi, T., Crosbie, M. (2011A) '*Cloud forensics: An overview*' Advances in Digital Forensics VII
6. Zawoad, Shams, and Ragib Hasan. "*Cloud forensics: a meta-study of challenges, approaches, and open problems*." arXiv preprint arXiv:1302.6312(2013).